Załącznik do Zarządzenia Nr 3a /2019
dyrektora Miejskiego Przedszkola Nr 6 w Legnicy z dnia 22.02.2019r.

PROCEDURA

POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW BEZPIECZEŃSTWA DANYCH W MIEJSKIM PRZEDSZKOLU SPECJALNYM NR 6 DLA DZIECI SŁABOWIDZĄCYCH W LEGNICY

SPIS TREŚCI

Rozdział 1

Postanowienia ogólne

§ 1

1. Instrukcja określa tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych lub powzięcia podejrzenia o takim naruszeniu.
2. Przestrzeganie postanowień niniejszej Instrukcji służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych oraz incydentów bezpieczeństwa danych w Miejskim Przedszkolu Specjalnym Nr 6 w Legnicy.
3. Użyte określenia i skróty oznaczają:
   1) MP – Miejskie Przedszkole
   2) ZOJO - Zespół Obsługi Jednostek Oświatowych w Legnicy;
   3) ADO - administrator danych osobowych - MP6 reprezentowane przez dyrektora;
   4) ATI - informatyk - osoba, której powierzono obowiązki związane z administrowaniem systemami teleinformatycznymi oraz zapewnieniem bezpieczeństwa systemów;
   5) SI - system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   6) Grupa Robocza art. 29 - grupa robocza ds. ochrony osób fizycznych powołana na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 r. Grupa została rozwiązana 25.05.2018 r. a w jej miejsce została powołana Europejska Rada Ochrony Danych;
   7) IOD - inspektor ochrony danych - osoba nadzorująca przestrzeganie zasad przetwarzania i ochrony danych osobowych w ZOJO;
   8) Intendent - pracownik, któremu w zakresie czynności powierzono dodatkowe zadania związane z ochroną danych osobowych;
   9) RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119);
   10) Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej);
   11) Jednostka obsługiwana – jednostka oświatowa wymieniona w § 2 ust. 1 statutu ZOJO stanowiącego załącznik do Uchwały nr XIX/186/12 Rady Miejskiej Legnicy z dn. 26.04.2012 r. w sprawie utworzenia Zespołu Obsługi Jednostek Oświatowych (ze. zm.)

Rozdział 2

Istota naruszenia danych osobowych

§ 2

1. Incydent związany z bezpieczeństwem informacji to pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań organizacji i zagrażają bezpieczeństwu informacji.
2. Naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Przyczyną naruszenia danych osobowych może być:
   1) wewnętrzne działanie niezamierzone;
   2) wewnętrzne działanie zamierzone;
   3) zewnętrzne działanie niezamierzone;
   4) zewnętrzne działanie zamierzone.

§3

1. Naruszeniem zasad organizacyjnej ochrony danych osobowych jest naruszenie środków, o których mowa w ust. 1 i 2 załącznika nr 1 do Polityki bezpieczeństwa danych osobowych w Miejskim Przedszkolu Specjalnym Nr 6 dla Dzieci Słabowidzących w Legnicy, w szczególności:
   1) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
   2) niezamykanie drzwi w przypadku opuszczenia pomieszczenia przez pracownika Miejskiego Przedszkola Specjalnego Nr 6 dla Dzieci Słabowidzących w Legnicy:
   3) pozostawianie klucza w drzwiach pomieszczenia, w którym przetwarzane są dane osobowe;
   4) praca przy przetwarzaniu danych osobowych osoby nieprzeszkolonej lub/i nieposiadającej upoważnienia do przetwarzania danych osobowych wydanego przez ADO;
   5) udzielenie informacji telefonicznych nieuprawnionej osobie do uzyskania tych informacji;
   6) przebywanie osób nieuprawnionych w pomieszczeniu gdzie przetwarza się dane osobowe bez nadzoru osoby upoważnionej przez ADO;
   7) celowe lub nieświadome przekazanie danych osobowych osobie nieuprawnionej do ich otrzymania;

8) nienależyte zabezpieczenie danych w tym nie chowanie dokumentów do zamykanych szaf i pozostawianie w miejscu ogólnie dostępnym, przechowywanie dokumentów i nośników cyfrowych zawierających dane osobowe w szafach z niesprawnymi zamkami;
9) wyrzucanie dokumentów zawierających dane osobowe bez uprzedniego ich zniszczenia w stopniu uniemożliwiającym odczytanie danych;
10) przebywanie pracowników obsługi informatycznej lub technicznej firm zewnętrznych w budynku bez nadzoru upoważnionego pracownika przedszkola ADO;
11) kradzież dokumentów lub nośników cyfrowych zawierających dane osobowe.

2. Naruszeniem zasad technicznej ochrony danych osobowych jest naruszenie środków, o których mowa w ust. 3 i 4 Załącznika nr 1 do Polityki bezpieczeństwa danych osobowych w Miejskim Przedszkolu Specjalnym Nr 6 dla Dzieci Słabowidzących w Legnicy, szczególności:
   1) naruszenie lub próby naruszenia integralności SI przez osoby nieuprawnione do dostępu do systemu informatycznego;
   2) nieautoryzowane logowanie do SI;
   3) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
   4) ujawnienia hasła funkcjonującego w SI osobie nieuprawnionej;
   5) istnienie nieautoryzowanych kont dostępu do SI, w tym nie blokowanie kont osób z cofniętym upoważnieniem do przetwarzania danych osobowych lub/i z cofniętym upoważnieniem do pracy w SI;
   6) włamanie lub próba włamania z zewnątrz sieci;
   7) nieautoryzowane zmiany danych w SI;
   8) nie zablokowanie komputera przez użytkownika przed opuszczeniem stacji roboczej;
   9) nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
   10) brak lub niepełna ochrona antywirusowa elementów systemu informatycznego;
   11) niewykonywanie kopii zapasowych w przewidzianym terminie;
   12) wykonywanie uszkodzonych kopii zapasowych;
   13) niewłaściwe lub nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe;
   14) brak zastosowania przy przekazywaniu danych z SI lub łączenia się z systemem informatycznym z zewnątrz kryptograficznych środków ochrony danych;
   15) zła jakość komunikacji w sieci telekomunikacyjnej.

§ 4

1. Zgodnie z opinią 03/2014 Grupy Roboczej art. 29 naruszenia ochrony danych osobowych można podzielić na trzy grupy:

1) naruszenie dostępu;
2) naruszenie integralności;
3) naruszenie tajemnicy (poufności).

2. W poniższej tabeli zestawiono wykaz naruszeń ochrony danych, które mogą występować w Miejskim Przedszkolu Specjalnym Nr 6 dla Dzieci słabowidzących w Legnicy, systematyzując je ze względu charakter. Lista naruszeń jest katalogiem otwartym, który okresowo podlegać będzie aktualizacji.

Charakter naruszeń		
Naruszenie dostępu	**Naruszenie integralności**	**Naruszenie tajemnicy**
1. Utrata nośnika danych USB z niezaszyfrowanymi danymi osobowymi.	1. Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania.	1. Osoba postronna informuje ADO o przypadkowym otrzymaniu danych osobowych jednego z jego klientów i przedstawia dowody niedozwolonego ujawnienia danych.
2. Zagubienie lub kradzież nośnika zawierającego kopię bazy danych klientów ADO.	2. Zmiana danych bez zgody osoby, której dane dotyczą.	2. ADO wykrywa, że mogło dojść do włamania do jego systemu. Sprawdza je i potwierdza, że miało to miejsce.
3. Jedyna kopia zbioru danych osobowych została zaszyfrowana przez oprogramowanie typu ransomware lub przez administratora przy użyciu klucza, który nie jest już w jego posiadaniu.	3. Pojawienie się złośliwego oprogramowania , które ingeruje w integralność danych.	3. Cyberprzestępca kontaktuje się z ADO po włamaniu się do jego systemu z żądaniem okupu. Po uprzednim sprawdzeniu systemu i potwierdzeniu, ADO ma jasne dowody że doszło do ataku.
4. Brak możliwości wykorzystania danych w założonym czasie, przez osobę do tego uprawnioną.		4. Nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów. Przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz starych plików. Nie usuwa jednak danych z dysku komputera).
5. Zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokalizacji dokumentacji papierowej, która zawiera dane osobowe.		5. Pojawienie się złośliwego oprogramowania , które ingeruje w poufność danych.
6. Nieuprawnione uzyskanie dostępu do informacji.		6. Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej poczcie elektronicznej, tj. drogą e-mailową lub za pomocą komunikatora internetowego (phishing).

7. Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń.		7. Nieprawidłowa anonimizacja danych osobowych w dokumencie.
8. Pojawienie się złośliwego oprogramowania, które ingeruje w dostępność danych.		8. Ustne ujawnienie danych osobowych.
9. Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do odbiorcy.		9. Niezamierzona publikacja danych osobowych.

§5

1. Naruszenie ochrony danych osobowych może powodować uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą, takie jak:
   - utrata kontroli nad własnymi danymi osobowymi;
   - ograniczenie możliwości realizowania przysługujących praw osobie której dane dotyczą (art. 15-22 RODO);
   - dyskryminacja;
   - kradzież lub sfałszowanie tożsamości;
   - strata finansowa;
   - nieuprawnione odwrócenie pseudonimizacji;
   - naruszenie dobrego imienia;
   - utratę poufności danych osobowych chronionych tajemnicą zawodową,

   lub wszelkie inne szkody:
   - gospodarcze;
   - społeczne.

Rozdział 3
Postepowanie w przypadku naruszenia ochrony danych

§ 6

1. W przypadku wystąpienia okoliczności wskazujących na możliwość naruszenia zasad ochrony danych, o którym mowa w § 3 pracownicy Miejskiego Przedszkola Specjalnego Nr 6 dla Dzieci słabowidzących w Legnicy zobowiązani są do natychmiastowego reagowania w sposób określony poniżej.
2. W sytuacji wskazującej na naruszenie ochrony danych osobowych należy:
   1) w miarę możliwości zabezpieczyć dane osobowe przed dalszą podatnością na naruszenie;

2) natychmiast poinformować swojego bezpośredniego przełożonego, ADO, IOD oraz dodatkowo
   a) w przypadku naruszenia zasad ochrony organizacyjnej zgłosić ten fakt do Intendenta, nauczyciela zastępującego dyrektora w przypadku jego nieobecności (dotyczy § 3 ust. 1 pkt 1, 2, 3, 4, 6, 8, 10, 11);
   b) w przypadku naruszenia zasad ochrony technicznej zgłosić ten fakt do Informatyka (dotyczy § 3 ust. 2 pkt 1, 2, 3, 4, 5, 6, 7,8, 9, 10, 11, 12, 13, 14, 15).

3. Po pierwszej reakcji na potencjalne naruszenie zasad ochrony danych osobowych, osoba stwierdzająca naruszenie wraz z kierownikiem komórki organizacyjnej, bądź nauczycielem zastępującym dyrektora, intendentem, ASI, Informatykiem (w zależności od sytuacji) oraz przy współpracy IOD zobowiązani są do:
   1) podjęcia czynności zmierzających do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów naruszenia i minimalizacji zaistniałych szkód, w szczególności poprzez:
      - wstrzymanie przekazywania i udostępniania danych osobowych;
      - usunięcie uchybień;
      - zastosowanie dodatkowych środków technicznych i organizacyjnych zabezpieczających dane osobowe;
      - zwiększenie kontroli podczas przetwarzania danych osobowych.
   2) możliwie pełnego udokumentowania zdarzenia celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.
   3) sporządzenie raportu z naruszenia ochrony danych według wzoru określonego w załączniku nr 1 do procedury.
4. ADO dokumentuje wszystkie naruszenia ochrony danych osobowych, w tym okoliczności zdarzenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania art. 33 RODO. W tym celu ADO prowadzi rejestr naruszeń ochrony danych osobowych lub incydentów bezpieczeństwa danych według wzoru określonego w załączniku nr 2 do procedury.

Rozdział 4

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 7

1. W sytuacji naruszenia zasad ochrony danych osobowych, niezwłocznie, po wcześniejszym wykonaniu czynności opisanych w § 6 ust. 2 i 3, dokonuje się oceny wagi naruszenia i oceny,

czy naruszenie skutkuje lub może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Oceny dokonuje zespół składający się z:
    - ADO;
    - IOD;
    - ASI/AIT/ jeśli naruszenie dotyczy danych osobowych przetwarzanych w systemie informatycznym.
3. Zespół winien dokonać oceny bez zbędnej zwłoki, nie później niż w terminie 48 godzin od stwierdzenia naruszenia. Określając poziomy naruszenia zespół posługuje się poniższym wzorem:

WN=KPD x PI + ON
gdzie: WN – Waga Naruszenia.
KPD – Kontekst Przetwarzania Danych.
PI- Prawdopodobieństwo Identyfikacji.
ON – Okoliczności Naruszenia.

KPD - Kontekst Przetwarzania Danych - KPD=A+B
gdzie: **A - rodzaj i poziom wrażliwości danych**:
- Dane podstawowe = 1,
- Dane (behawioralne) dotyczące zachowań osoby = 2 (pozwalające ustalić preferencje, radzenia sobie w nietypowych sytuacjach, status społeczny),
- Dane finansowe = 3 (mające związek z saldami, transakcjami, nr kont),
- Dane szczególnych kategorii = 4.

B - kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę:
- Szeroki zakres danych/wolumen danych (+) np cześć dysku „partycja", krążek SD lub DVD, pendrive, skompresowany plik,
- Charakter danych (+/-),
- Specyfika podmiotu danych lub administratora (+/-),
- Możliwe negatywne skutki dla podmiotu danych (+),
- Publiczna dostępność danych przed naruszeniem (-),
- Nieważność danych (-).

PI - Prawdopodobieństwo Identyfikacji:
- Znikome = 0,25,
- Ograniczone = 0,5,
- Wysokie = 0,75,
- Maksymalne = 1.

ON - Okoliczności Naruszenia:
Naruszenie Poufności – Dane ujawnione:
- Znanym odbiorcom (+0,25),
- Nieznanej liczbie odbiorców danych (+0,5).

Naruszenie Integralności – Dane zmienione i:
- Możliwe jest ich odzyskanie (+0,25),
- Brak jest możliwości ich odzyskania (+0,5).

Naruszenie Dostępności – Niedostępność danych:
- Czasowa (+0,25),
- Pełna i brak możliwości ich odzyskania przez ADO lub podmiot danych (+0,5).

Intencjonalne działanie sprawcy - celowe, umyślne, zamierzone (+0,5).

Po ustaleniu wyniku wagi naruszenia dokonuje się jego oceny poprzez zestawienie z poniższa tabelą:

Wynik	Waga naruszenia	Opis
WN<2	**Niska**	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<=WN<3	**Średnia**	Osoby mogą dotknąć niedogodności, które są możliwe do pokonania
3<=WN<4	**Wysoka**	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=WN	**Bardzo wysoka**	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

Przykład oceny wagi naruszenia znajduje się w załączniku nr 3 do procedury.

§ 8

1. W przypadku naruszenia ochrony danych osobowych, do którego wyliczona waga naruszenia będzie większa niż niska ADO bez zbędnej zwłoki (w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia) zgłasza je (zgodnie z art. 33 RODO) do UODO. Jeżeli

   – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można jej udzielać sukcesywnie bez zbędnej zwłoki. Wzór zgłoszenia naruszenia ochrony danych osobowych zawiera załącznik nr 4 do procedury.
2. Zgłoszenie naruszenia ochrony danych musi co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. W Miejskim Przedszkolu Specjalnym Nr 6 dla Dzieci Słabowidzących w Legnicy występują następujące kategorie osób (zgodnie z „Wytycznymi Grupy Roboczej art. 29”):
   1) pracownicy,
   2) inne osoby zatrudnione,
   3) byli pracownicy,
   4) emeryci i renciści,
   5) kontrahenci,
   6) rodzice
   7) dzieci
5. W przypadku podjęcia decyzji o niezgłoszeniu naruszenia do UODO administrator dokumentuje przyczyny, dla których uważa, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych. Jeżeli administrator uzna, że spełniony jest któryś z warunków opisanych w §11 ust 3 niniejszej procedury (art. 34 ust. 3 RODO), powinien być w stanie przedstawić odnośne dowody.

§ 9

1. IOD jest odpowiedzialny za analizę incydentów bezpieczeństwa danych oraz naruszenia ochrony danych osobowych. Źródłami informacji o incydentach, zagrożeniach lub słabościach są:

1) zgłoszenia od:
   - ADO;
   - pracowników;
   - osób których dane osobowe są przetwarzane.
2) wyniki kontroli.

2. IOD odgrywa kluczową rolę w zapobieganiu lub przygotowywaniu się na naruszenia, udzielając porad i monitorując przestrzeganie przepisów, a także gdy dojdzie do naruszenia (tj. przy zgłaszaniu go organowi nadzorczemu) oraz podczas wszelkich dalszych postepowań przez organ nadzorczy. IOD powinien być niezwłocznie informowany o zaistnieniu naruszenia tak aby mógł właściwie
   i poprawnie nadzorować cały proces zarzadzania naruszeniem i zgłaszania go do UODO.

Rozdział 5

Obowiązki ZOJO jako podmiotu przetwarzającego w zakresie zgłoszenia naruszenia

§ 10

1. ZOJO jako podmiot, któremu powierzono przetwarzanie danych osobowych, po stwierdzeniu ich naruszenia, bez zbędnej zwłoki ale nie później niż w ciągu 48 godzin zgłasza ten fakt administratorowi danych osobowych – dyrektorowi jednostki obsługiwanej (art. 33 ust. 2 RODO). Czas od stwierdzenia naruszenia do przekazania pełnej informacji powinien być jak najkrótszy, by gwarantował administratorowi wywiązanie się z obowiązku zgłoszenia naruszenia do UODO w ciągu 72 godzin od wystąpienia zdarzenia w ZOJO.
2. W sytuacji wystąpienia naruszenia wymagającego dłuższej procedury wyjaśniającej, ZOJO natychmiast zgłasza naruszenie dyrektorowi jednostki obsługiwanej, a następnie sukcesywne przekazuje informacje, gdy stają się one dostępne.
3. ZOJO wspiera administratora danych osobowych jednostki obsługiwanej w realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych UODO i zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych, udzielając wszelkich wyjaśnień administratorowi danych osobowych jednostki obsługiwanej.
4. ZOJO może dokonać zgłoszenia w imieniu administratora, jeżeli nadał mu odpowiednie upoważnienie i jest to przewidziane w umowie pomiędzy administratorem a podmiotem przetwarzającym. Zgłoszenia należy wówczas dokonać zgodnie z art. 33 i 34. Należy jednak pamiętać, że odpowiedzialność prawna za zgłoszenie spoczywa na administratorze.
5. Jeżeli zdarzenie może mieć wpływ na naruszenie danych osobowych wielu jednostek obsługiwanych, wówczas ZOJO zawiadamia o naruszeniu każdego z administratorów tych danych.

Rozdział 6

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§ 11

1. Jeżeli naruszenie ochrony danych osobowych może powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu zgodnie z art. 34 RODO.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych zgodnie z art. 33 ust. 3 lit b), c), d) RODO.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt 1;
   3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

WYKAZ ZAŁĄCZNIKÓW

Załącznik Nr 1 – Raport z naruszenia ochrony danych

Załącznik Nr 2 – Rejestr naruszeń ochrony danych osobowych lub incydentów bezpieczeństwa danych

Załącznik Nr 3 – Ocena wagi naruszenia ochrony danych osobowych

Załącznik Nr 4 – Zgłoszenie naruszenia ochrony danych osobowych

Załącznik nr 1
do Procedury postepowania
w sytuacji naruszenia
ochrony danych osobowych

Raport z naruszenia ochrony danych

1. Data i czas stwierdzenia naruszenia

……..……..…….

2. Sposób stwierdzenia naruszenia

…….

3. Data i czas zaistnienia naruszenia ……..

4. Data i czas zakończenia naruszenia

……

5. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

……

……

6. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

……

……..……..

7. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……

……..……..

……..……..

8. Podjęte działania:

……..……

……..

9. Wstępna ocena przyczyn wystąpienia naruszenia:

……..……

……..

10. Postępowanie wyjaśniające i naprawcze:

……

……..……..

…… ……
(data i podpis pracownika ……) (data i podpis ADO)

……
(data i podpis IDO)

Rejestr naruszeń ochrony danych osobowych lub incydentów bezpieczeństwa danych (art. 33 ust. 5)

Data otrzymania informacji	Opis /okoliczności naruszenia ochrony danych osobowych lub incydentu *	Źródło zgłoszenia	Konsekwencje naruszenia ochrony danych osobowych/incydentu	Działania korygujące/ Zapobiegawcze **	Ocena skuteczności przyjętych rozwiązań	Data zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych ***	Data przekazania informacji o incydencie do osoby, której danych dotyczą	Uwagi

* opisać charakter naruszenia ochrony danych osobowych w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób, których dane dotyczą.

** opisać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki celu zminimalizowania jego ewentualnych negatywnych skutków. Należy podać termin rozpoczęcia i zakończenia wdrożenia działań.

*** w tym przyczyny opóźnienia w zgłoszeniu dokonywanym do organu nadzorczego (UODO).

Ocena wagi naruszenia ochrony danych osobowych

Zdarzenie	zagubienie niezaszyfrowanego pendrive z listą 150 uczestników konferencji dla rodziców dzieci chorych na ……
Zakres danych	imię, nazwisko, e-mail

Wyliczenie wagi naruszenia

WN=KPD x PI + ON

KPD=A+B – kontekst przetwarzania danych

A - rodzaj i poziom wrażliwości danych
A = 1 - dane podstawowe

B - kontekst przetwarzania
B = 2 - specyfika administratora
- możliwe negatywne skutki dla podmiotu danych
KPD = 3

PI – prawdopodobieństwo identyfikacji
PI = 1- poziom identyfikacji maksymalny

ON= NP+NI+ND+IDS – okoliczności naruszenia

NP - naruszenie poufności
NP = 0,5 – nieznana liczba odbiorców

NI - naruszenie integralności
NI = 0 – nie zmieniono danych

ND – **naruszenie dostępności**
ND - 0,25 – czasowa niedostępność

IDS – **intencjonalne działanie sprawcy**
IDS – 0 – niecelowe działanie

ON = 0,5+0+0,25+0 =0,75

WN=KPD x PI + ON = 3x1+0,75=3,75

3,75 – wysoka waga naruszenia **- naruszenie należy zgłosić do UODO**

Załącznik nr 4
do Procedury postepowania
w sytuacji naruszenia
ochrony danych osobowych

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.

☉ **Zgłoszenie kompletne/jednorazowe**	☐ **Zgłoszenie wstępne**	☐ **Zgłoszenie uzupełniające/zmieniające**
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić datę.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie)	Podaj numer.	NIP (opcjonalnie)	Podaj numer.	KRS (opcjonalnie)	Podaj numer.

Sektor (opcjonalnie) *Dla sektora publicznego:* Wpisz nazwę sektora *Dla sektora prywatnego:* Wpisz nazwę sektora

2B. Adres siedziby administratora danych

Ulica	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer	Numer lokalu	Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.		
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Powiat	Kliknij tutaj, aby wprowadzić tekst.		
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Państwo	Kliknij tutaj, aby wprowadzić tekst.		

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
4.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
5.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** (zgodnie z art. 33a KPA) oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko	imię i nazwisko.	Numer telefonu	Numer telefonu.	Adres e-mail	E-mail.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
2.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
3.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
4.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

- ☐ Zgubienie lub kradzież nośnika/urządzenia
- ☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
- ☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy
- ☐ Nieuprawnione uzyskanie dostępu do informacji
- ☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
- ☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
- ☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)
- ☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie
- ☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
- ☐ Niezamierzona publikacja
- ☐ Dane osobowe wysłane do niewłaściwego odbiorcy
- ☐ Ujawnienie danych niewłaściwej osoby
- ☐ Ustne ujawnienie danych osobowych

4C. Przyczyna naruszenia

- ☐ Wewnętrzne działanie niezamierzone
- ☐ Wewnętrzne działanie zamierzone
- ☐ Zewnętrzne działanie niezamierzone
- ☐ Zewnętrzne działanie zamierzone

4D. Charakter

- ☐ Naruszenie poufności danych

  Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych
- ☐ Naruszenie integralności danych

  Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania
- ☐ Naruszenie dostępności danych

  Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4E. Dzieci

- ☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których mogło dotyczyć naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- ☐ Nazwiska i imiona
- ☐ Imiona rodziców
- ☐ Data urodzenia
- ☐ Numer rachunku bankowego
- ☐ Adres zamieszkania lub pobytu
- ☐ Numer ewidencyjny PESEL
- ☐ Adres e-mail
- ☐ Nazwa użytkownika i/lub hasło
- ☐ Dane dotyczące zarobków i/lub posiadanego majątku
- ☐ Nazwisko rodowe matki
- ☐ Seria i numer dowodu osobistego
- ☐ Numer telefonu
- ☐ Wizerunek
- ☐ Inne, wskaż jakie:

Kliknij tutaj, aby wprowadzić tekst.

6B. Dane szczególnej kategorii

- ☐ Dane o pochodzeniu rasowym lub etnicznym
- ☐ Dane o poglądach politycznych
- ☐ Dane o przekonaniach religijnych lub światopoglądowych
- ☐ Dane o przynależności do związków zawodowych
- ☐ Dane dotyczące seksualności lub orientacji seksualnej
- ☐ Dane dotyczące zdrowia
- ☐ Dane genetyczne
- ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

6C. Dane, o których mowa w art. 10 RODO

- ☐ Dane dotyczące wyroków skazujących
- ☐ Dane dotyczące czynów zabronionych
- ☐ Inne

Kliknij tutaj, aby wprowadzić tekst.

7. Kategorie osób

- ☐ Pracownicy
- ☐ Użytkownicy
- ☐ Subskrybenci
- ☐ Studenci
- ☐ Uczniowie
- ☐ Służby mundurowe (np. wojsko, policja)
- ☐ Klienci (obecni i potencjalni)
- ☐ Klienci podmiotów publicznych
- ☐ Pacjenci
- ☐ Dzieci
- ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie:
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- ☐ Utrata kontroli nad własnymi danymi osobowymi
- ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- ☐ Ograniczenie możliwości realizowania praw
- ☐ Dyskryminacja
- ☐ Kradzież lub sfałszowanie tożsamości
- ☐ Strata finansowa
- ☐ Naruszenie dobrego imienia
- ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

8B. Ryzyko naruszenia praw i wolności osób fizycznych

○ Niskie ○ Średnie ◉ Wysokie

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

10. Zawiadamianie osób, których dane dotyczą

Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

◉ Tak

○ Nie, ale zostaną zawiadomione

Pamiętaj, że po zawiadomieniu osób, należy przesłać treść zawiadomienia do UODO.

○ Nie, nie zostaną zawiadomione

○ Nie oceniłem jeszcze

Czy indywidualnie?

◉ Tak

○ Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymag niewspółmiernie dużego wysiłku. W związku z tym został wydany publiczny kon lub zastosowano podobny środek, za pomocą którego osoby, których dane dot zostały poinformowane w równie skuteczny sposób.

Wskaż datę kiedy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

Wskaż datę kiedy zamierzasz zawiadomić osoby, których dane dotyczą, o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

☐ Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą

Liczba zawiadomionych osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

Powód niezawiadomienia osób, których dane dotyczą:

○ Przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

○ Po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

11. Przetwarzanie transgraniczne i inne powiadomienie

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry
☐ Wielka Brytania	☐ Włochy		

☐ Naruszenie zostało lub zostanie zgłoszone innemu organowi ochrony danych osobowych (opcjonalnie)

Wymień inne organy nadzorcze ochrony danych osobowych, którym naruszenie zostało lub zostanie zgłoszone

Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu z powodu innych zobowiązań prawnych (opcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

Kliknij tutaj, aby wprowadzić tekst.

_____

Data, miejscowość
(dla zgłoszenia w formie papierowej)

_____

Podpis osoby lub osób upoważnionych do reprezentowania administratora[1]
(dla zgłoszenia w formie papierowej)

[1] Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa